



UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF INSPECTOR GENERAL
Washington D.C. 20250



February 27, 2007

REPLY TO

ATTN OF: 50501-8-FM

TO: David M. Combs
Chief Information Officer
Office of the Chief Information Officer

Kevin Brown
Deputy Chief for Management
Natural Resources Conservation Service

Sherie Hinton-Henry
Deputy Administrator
for Operations Management
Rural Development

Teresa C. Lasseter
Administrator
Farm Service Agency

FROM: Robert W. Young /s/
Assistant Inspector General
for Audit

SUBJECT: Information Technology – Stolen Computer Equipment Containing
Sensitive Information

We have completed our review of the Department of Agriculture's (USDA) controls over stolen computer equipment for the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) at the Information Technology Services (ITS) field sites. This letter represents the results of our review. Our objective was to determine, to the extent possible, what information resided on the stolen computers and what sensitive information currently resides on the existing computers.

We found that controls over stolen computer equipment were lacking in FSA, NRCS, RD, and ITS. Specifically, we found that Privacy Act/Sensitive information was stored on computers that were stolen. In addition, the agencies did not notify the individuals whose information may

have been compromised. These agencies lacked policies and procedures to adequately notify proper authorities and affected parties when thefts of computer equipment occurred. Prior to a June 23, 2006, Office of Management and Budget (OMB) memorandum requiring improved security over sensitive information, Office of the Chief Information Officer (OCIO) had provided agencies limited guidance on actions to take if computers were lost or stolen. OCIO did provide additional direction to the agencies after the OMB issuance, but the guidance still was not specific on procedures to determine whether personally identifiable information was contained on the computers. As a result, personally identifiable information of USDA customers and employees may have been lost and is at risk for improper use.

BACKGROUND

During recent months, the disclosure or theft of Privacy Act/Sensitive information has received renewed attention within the Government. A high profile theft of equipment carrying millions of Privacy Act/Sensitive records led the OMB to issue new mandates on securing this type of information. On June 23, 2006, OMB issued Memorandum M-06-16, "Protection of Sensitive Agency Information," which required agencies to encrypt information, within 45 days, on all mobile computers/devices which carry agency information unless the information is determined to be non-sensitive. In addition, OCIO has issued several memorandums concerning lost or stolen computer equipment. In a June 27, 2006, memorandum, OCIO required agencies to review lost or stolen items containing sensitive information and report it as an incident. We noted that the agencies in our review had reported back to OCIO that computer equipment had been stolen but it was unknown as to whether Privacy Act/Sensitive information was on the computers.

OBJECTIVE

The primary objective was to determine, to the extent possible, what information resided on the stolen computers and what sensitive information currently resides on the existing computers.

SCOPE

Our scope was computers reported stolen at the subject agencies from October 1, 2005, through May 31, 2006. We obtained a listing of stolen computers from ITS. ITS did not track, report and monitor these items, but generated the listing after we requested it. In total there were 95 pieces of computer equipment on the list. Exhibit A documents our sample of locations visited and where phone interviews were conducted.

METHODOLOGY

We interviewed IT specialists and computer users at the locations contained in Exhibit A. In addition, we downloaded directory information from the ITS Large Office in Kansas City,

Missouri, in an attempt to identify file names that could indicate the presence of Privacy Act/Sensitive information.

RESULTS

In a July 25, 2006, letter to Congress, USDA reported only eight incidents of Privacy Act/Sensitive information that had been compromised since 2003. Our review showed that USDA's report to Congress was not accurate and that the true number of incidents may not be known because of inadequate guidance requiring agencies to track and report information on stolen computer equipment. As evidenced in our review, we found nine additional incidents of compromised Privacy Act/Sensitive information in the limited 8-month scope of our review.

Prior to the OMB memorandum, OCIO had provided limited guidance on what agencies were required to do when equipment was stolen and/or lost. Agencies were not tracking, reporting, or following up on stolen or lost equipment. The lack of guidance and procedures led to the inaccurate reporting to Congress, as noted above. ITS did not track, monitor, and report on stolen computer equipment and only generated a list of the equipment based upon our request. Since our request for the stolen item list, OCIO has issued some guidance to agencies and drafted internal procedures on how to handle stolen or lost computer equipment. However, OCIO had not issued Departmentwide guidance addressing agency requirements for tracking and reporting lost and stolen computers and for determining the types of information stored on the computers.

We began our review by examining the stolen computer spreadsheet provided by ITS. In total, there were 95 computers stolen from October 1, 2005, through May 31, 2006. We judgmentally selected a sample of 66 of the 95 stolen computers at 9 service center locations throughout the country. Our sample selection was based upon multiple computers being stolen at a site and the site locations. We interviewed the users of the computers to determine if they knew whether Privacy Act/Sensitive information was on the computers when the devices were stolen. In addition, we scanned current computers at the locations to determine whether Privacy Act/Sensitive information was presently on the equipment to determine the likeliness of this information being present when similar equipment was stolen. We noted:

- 9 instances where the user was aware of Privacy Act/Sensitive information present on the machine when it was stolen. Information on the lost computers included producer/borrower names, addresses, social security numbers, and payment information;
- 55 instances where the user was unaware of followup by the agency or OCIO to determine if Privacy Act/Sensitive information was actually on the stolen computer;
- 7 instances where external storage devices were stolen along with the computer and the users said that there was no Privacy Act/Sensitive information on any of the equipment;
- 66 instances where no encryption was present on the computer;

- 26 instances where the users were not aware of any policies or procedures regarding stolen equipment; and
- 27 instances where users were not aware whether the theft was reported to the Office of Inspector General.

Agency information technology personnel all stated that Privacy Act/Sensitive information was not stored on the computers, but was stored on the server. Our review disclosed that this was not the case. For example, one agency downloaded Privacy Act/Sensitive information onto the laptop/desktop computers and then uploaded this information to the server once the user was finished with the information. However, a flaw in the programming did not always delete the information from computers when the information was uploaded. Our scan of current equipment at our sample locations disclosed over 2,000 files of Privacy Act/Sensitive information on the computers during the time of our scanning. This information included producer names, addresses, social security numbers, and payment information similar to what we found during our testing. The agency has since stated that the programming flaw has been fixed.

There were limited controls in place to ensure that users do not download Privacy Act/Sensitive information from the server onto the computers. Although the default setting on computers is to store all information on the server, the user can change the default at anytime he/she saves a file. The information that is stored on the server or is accessed over the internet can leave Privacy Act/Sensitive information on the local machine. Items such as Temporary Internet Files, Recycle Bins, Virtual Memory, and unallocated space could allow a knowledgeable individual to retrieve this information.

OCIO must rely on the agency's due diligence in tracking and reporting computer equipment that has been stolen, as well as in determining whether the equipment may have contained Privacy Act/Sensitive information. Until Departmentwide encryption is effectively enforced, OCIO cannot be assured that all information is adequately secured and protected. Since the audit was completed, it appears that the Department has made efforts to improve the tracking, reporting and monitoring of stolen equipment.

In response to the data call, we were told by the OCIO (see exhibit B) that many agency officials could not confirm whether or not Privacy Act/Sensitive information existed on the lost or stolen equipment, primarily because of the length of time that had lapsed since the incident occurred. As a result, OCIO did not rely on the oral testimony of employees when it could not be confirmed exactly what type of information was stored on those systems. We confirmed from the employees that Privacy Act/Sensitive information was in fact on the stolen computers. *Government Auditing Standards* affirms that oral testimony is an acceptable form of evidence. Also, asking the user of the computer what type of information was on a computer at the time of the theft is the only logical way to determine what could have been on the computer that has yet to be recovered. OIG stands firm that this is not only acceptable evidence, it is the only evidence that is available.

RECOMMENDATIONS

1. FSA, NRCS, RD, and ITS need to effectively encrypt the entire hard drive and removable media on all desktops and laptops to ensure that Privacy Act/Sensitive information is not compromised due to stolen or lost equipment. Mobile computing devices should also be physically secured.

Agency Response. OCIO-ITS agreed with the recommendation and stated that they are working towards the goal of encrypting the entire hard drive. They have evaluated products to accomplish this and expect a Blanket Purchase Agreement to be in place by March 31, 2007. They anticipate completing the encryption solution by December 2007. In addition, they have already issued guidance to the agencies on steps that can be taken to encrypt files for an interim solution.

OIG Position. We concur with the actions outlined in OCIO-ITS response. However, in order to reach management decision, please provide a detailed, time phased plan to accomplish implementation of the solution throughout the country.

2. FSA, NRCS, RD, and ITS need to develop effective policies and procedures to notify the OCIO, OIG, and potential affected parties when equipment is stolen and/or lost.

Agency Response. The OCIO-ITS agreed with the recommendation. OCIO-ITS stated that they are in the process of reviewing and updating the current OCIO-ITS policy and procedures relating to incident handling in accordance with Departmental and NIST guidance.

OIG Position. We concur with the actions outlined in the OCIO-ITS response. However, in order to reach management decision, please provide a detailed, time phased plan for the completion of the policies and procedures.

3. OCIO needs to implement Departmentwide guidance regarding tracking and reporting requirements for computer equipment that is stolen or lost. This should include procedures for determining whether the subject equipment may have contained Privacy Act/Sensitive information.

Agency Response. The OCIO-ITS agreed with the recommendation. After the OIG Audit and OMB Memos, the OCIO issued additional incident tracking guidance to the agencies.

OIG Position. We concur with OCIO-ITS management decision on this recommendation.

4. OCIO should develop a process to verify agency data before relying on it.

Agency Response. This recommendation was added after the exit conference and the OCIO has not officially responded.

OIG Position. In order to reach management decision on this recommendation, the OCIO needs to provide a detailed, time phased plan when the policies and procedures to verify agency submitted data will be done.

cc:

Audit Liaison Officers for:

Office of the Chief Information Officer
Natural Resources Conservation Service
Rural Development
Farm Service Agency

Exhibit A – Sample Sites

Location of Service Center	Number of Computers Reported as Stolen
Tangent, Oregon	23
Colorado Springs, Colorado	9
Arlington, Texas	9
Avondale, Arizona	7
Yuba City, California	6
Stockton, California	4
Frederick, Maryland	3
Renton, Washington	3
Caldwell, Idaho	2
Total	66



FEB 7 2007

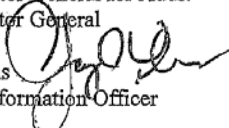
United States
Department of
Agriculture

Office of the Chief
Information Officer

1400 Independence
Avenue SW

Washington, DC
20250

TO: Robert W. Young
Assistant Inspector General for Audit
Office of Inspector General

FROM: Jerry E. Williams 
Deputy Chief Information Officer

SUBJECT: Response to Review 50501-8-FM, Information Technology –
Stolen Equipment Containing Sensitive Information

The Office of the Chief Information Officer (OCIO) has reviewed the results of the recent Office of the Inspector General (OIG) review 50501-8-FM, "Information Technology – Stolen Computer Equipment Containing Sensitive Information." This office recognized that lost and stolen equipment was not being properly tracked or reported to the proper authorities, and, in June 2006, we conducted a data call of all lost and stolen equipment from all agencies. Further, on June 27, 2006, David Combs instructed all agencies to report all lost and stolen equipment to Cyber Security as a security incident. Since that memorandum, Cyber Security has been following its incident response procedures for all lost and stolen equipment, including reporting such incidents to US-CERT.

In response to OCIO data call, many agency officials could not confirm whether or not Personally Identifiable Information (PII) data existed on the lost or stolen equipment, primarily because of the length of time that had lapsed since the incident occurred. As a result, we did not rely on the oral testimony of employees when it could not be confirmed exactly what type of information was stored on those systems. All nine of these instances occurred before this office instituted the reporting requirements and therefore were not captured in our incidents database. Finally, we cannot identify any legislative or department requirements that at the time those incidents occurred required the central reporting of the information.

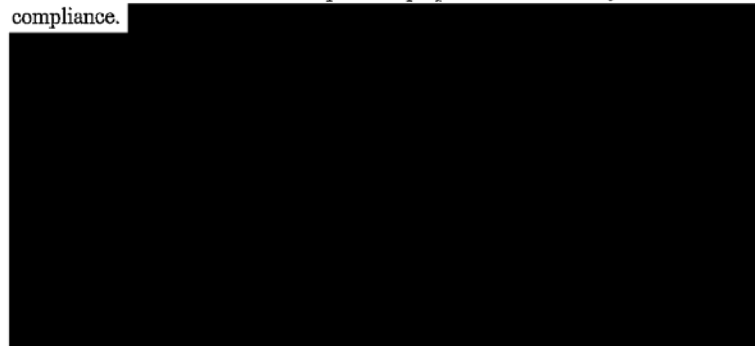
Your report states that our memorandum to Congress dated July 25, 2006, was not complete and inaccurate since you identified at least nine additional instances of PII on lost or stolen laptops. In our July memorandum to Congress, we reported only verified instances of lost or stolen PII information. Therefore, we request that you indicate within the text of your report that your determination that PII information had been exposed was based on the oral testimony of employees several months, or perhaps over a year, after the incident occurred.

Finally, your report states that OCIO-Information Technology Services (ITS) was not tracking lost and stolen equipment, yet OCIO-ITS was able to produce a report from their database of all lost and stolen equipment. Your report should note that the report came from OCIO-ITS' inventory system where lost and stolen equipment was noted. If OIG believes this is not sufficient for tracking lost and stolen equipment, OIG should make a recommendation addressing this weakness.

Our ability to remediate all findings is dependent on the availability of funds. OCIO operates the infrastructure for all the service center agencies and is now in the process of identifying resources and anticipated budget items. Since OCIO-Information Technology Services (OCIO-ITS) is funded through a Working Capital Fund, we will be presenting additional budgetary requirements to the Service Center Agencies (SCAs) for the remediation of these findings in fiscal year 2007.

Recommendation Number 1: FSA, NRCS, RD, and ITS need to effectively encrypt the entire hard drive and removable media on all desktops and laptops to ensure that Privacy Act/Sensitive information is not compromised due to stolen or lost equipment. Mobile computing devices should also be physically secured.

OCIO agrees with the recommendation to encrypt effectively the entire hard drive and removable media on all desktops and laptops to ensure Privacy Act compliance.



During fiscal year 2006, OCIO Cyber Security (OCIO-CS) coordinated an encryption solution study in which OCIO-ITS participated. OCIO evaluated several products that provided whole disk encryption, and rated each solution based on the following: meeting National Institute of Standards and Technology encryption requirements, level of effectiveness, ease of use, and centralized administration capabilities. It is anticipated that an award of a Blanket Purchase Agreement for selected whole disk encryption products will occur in the second quarter of fiscal year 2007. Once this purchase agreement is in place and funding becomes available, OCIO-ITS will pursue a more robust encryption solution. We anticipate having this solution in place by December 2007.

OCIO will work with the SCA's to effectively implement controls to physically secure mobile computing devices assigned to federal employees and contractors.

Recommendation Number 2: FSA, NRCS, RD, and ITS need to develop effective policies and procedures to notify the OCIO, OIG, and potential parties when equipment is stolen and/or lost.

OCIO-ITS agrees with the recommendation to develop effective policies and procedures to notify the OCIO, OIG, and potential parties when equipment is stolen and/or lost. Several events during the last year resulted in OCIO re-evaluating processes and updating procedures including the response time requirements. However, OCIO-ITS does not differ in this distinction of re-evaluation of the stolen equipment processes based on additional scrutiny that came about in 2006.

Stolen equipment was recorded by OCIO-ITS within Magic as EATS/Stolen Equipment and reported to the appropriate SCA ISSPM. OCIO-ITS, in compliance with the memorandum from USDA CIO, Dave Combs, dated June 27, 2006, began reporting stolen equipment incidents to OCIO-CS. It should be noted that OCIO-ITS stolen equipment processes have always included a requirement to report to local law enforcement agencies. Completion of a local police report is required.

OCIO-ITS is in the process of reviewing and updating the current OCIO-ITS policy and procedures relating to Incident Handling in accordance with Department and NIST guidelines. All recommended changes to OCIO-ITS Policy and Procedures will be submitted to OCIO-ITS Security Policy Branch for review and concurrence. In addition, OCIO will work with the SCA's to ensure that the policies and procedures will be made into a Departmental Regulation and be applicable to them.

Recommendation Number 3: OCIO needs to implement Department wide guidance regarding tracking and reporting requirements for computer equipment that is stolen or lost. This should include procedures whether the subject equipment may have contained Privacy Act/Sensitive information.

OCIO concurs with this recommendation and had already issued guidance on June 27, 2006 on reporting lost or stolen equipment, especially equipment which stores PII data. OCIO-CS has issued incident handling procedures that have been expanded to include the recording and tracking of lost or stolen equipment on January 29, 2007. Lost and stolen equipment is also reported to US-CERT within one hour of notification to ensure timely reporting in the event that the equipment does have PII or other sensitive information as required by OMB 06-16. OCIO-CS is also updating the Department Regulation on incident response and plans to accomplish this by September 30, 2007.

If you have any questions regarding the above responses, please contact Greg Gage, OCIO-ITS Information Systems Security Program Manager at greg.gage@wdc.usda.gov or (202) 720-8650 or Steven Bryce Eckland, OCIO-CS

Informational copies provided to:

Sherry Linkins
Audit Liaison Officer
Office of the Chief Information Officer

Dan Runnels
Director of Operations Management
and Oversight Division
Natural Resources Conservation Service

John Dunsmuir
Acting Director
Financial and Management Division

T. Mike McCann
Operations Review and Analysis Staff